UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/711,433	09/17/2004	Mark Merkow	03292.102050.	5432

66569 7590 05/27/2009
FITZPATRICK CELLA (AMEX)
30 ROCKEFELLER PLAZA
NEW YORK, NY 10112

EXAMINER	
FEARER, MARK D	

ART UNIT	PAPER NUMBER
2443	

MAIL DATE	DELIVERY MODE
05/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/711,433	MERKOW ET AL.	
	Examiner	Art Unit	
	MARK D. FEARER	2443	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1- 2, 9-13 and 15-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1- 2, 9-13 and 15-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's Amendment filed 02 March 2009 is acknowledged.
2. Claims 17-20, and 23 have been amended.
3. Claim 6 is cancelled.
4. Claims 1- 2, 9-13 and 15-25 are pending in the present application.
5. This action is made FINAL.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any

evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

7. Claims 1, 9-10, 13, 16-17, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gullotta et al. (US 6985955 B2) in view of Muhlestein et al. (US 20030195942 A1).

.

Consider claims 1 and 16. Gullotta et al. discloses a computer implemented method for dynamically provisioning computing resources, said method comprising: receiving a request for a computing resource, wherein said request is associated with an asset; determining an asset classification of said asset, a business value of said asset, and a resource classification related to said asset (column 7 lines 45-52), wherein said asset classification is at least one of: a public asset, a business confidential asset, a private asset, and a secret asset, wherein said business value of said asset is one of: a low value, a medium value, and a high value (column 18 lines 19-32), and wherein said resource classification is one of: a trusted classification for internal entities and a non-trusted classification for external entities (column 14 lines 3-18); and provisioning said computing resource based on said determining step (column 5 lines 13-35, column 18 lines 34-46, column 11 lines 24-52, and column 12 lines 34-53). However, Gullotta et al. fails to disclose a computer implemented method for

dynamically provisioning computing resources wherein an asset is assigned to one of a plurality of security domains based on a determining step, wherein each security domain corresponds to a respective degree of security control; and provisioning a computing resource based on said one of said plurality of security domains. Muhlestein et al. discloses a method and apparatus for encapsulating a virtual filer on a filer wherein each vfiler is assigned to a distinct domain ((“Specifically, each vfiler is allocated a certain amount, i.e., a subset, of dedicated and distinct units of storage resources, and one or more dedicated and distinct network addresses. Each vfiler is also allowed shared access to the common file system on behalf of its client. Therefore, interpretations of a security object associated with, e.g., a client accessing the common file system may vary among vfilers. To address this, each vfiler is provided a vfiler context data structure (hereinafter "vfiler context") including, among other things, information pertaining to a unique and distinct security domain of the vfiler to thereby enable controlled access to allocated and shared resources of the vfiler. For example, the vfiler context of a first vfiler ensures that users or clients of a first security domain can use a first set of source and destination network addresses when issuing requests to access a first subset of storage resources on the filer. Similarly, the vfiler context of a second vfiler ensures that clients of a second security domain may use a second set of source and destination network addresses to access a second subset of storage resources. Notably, the clients of each security domain are unaware of each other's "presence" on the filer and, further, are unable to access each other's storage resources. In sum, no data flow exists between vfilers.”) paragraphs 0058-0059).

Gullotta et al. discloses a prior art computer implemented method for dynamically provisioning computing resources, said method comprising: receiving a request for a computing resource, wherein said request is associated with an asset; determining an asset classification of said asset, a business value of said asset, and a resource classification related to said asset, wherein said asset classification is at least one of: a public asset, a business confidential asset, a private asset, and a secret asset, wherein said business value of said asset is one of: a low value, a medium value, and a high value, and wherein said resource classification is one of: a trusted classification for internal entities and a non-trusted classification for external entities; and provisioning said computing resource based on said determining step upon which the claimed invention can be seen as an improvement.

Muhlestein et al. teaches a prior art comparable method and apparatus for encapsulating a virtual filer on a filer wherein each vfiler is assigned to a distinct domain.

Thus, the manner of enhancing a particular device (method and apparatus for encapsulating a virtual filer on a filer wherein each vfiler is assigned to a distinct domain) was made part of the ordinary capabilities of one skilled in the art based upon the teaching of such improvement in Muhlestein et al. Accordingly, one of ordinary skill in the art would have been capable of applying this known "improvement" technique in the same manner to the prior art computer implemented method for dynamically provisioning computing resources, said method comprising: receiving a request for a computing resource, wherein said request is associated with an asset; determining an

asset classification of said asset, a business value of said asset, and a resource classification related to said asset, wherein said asset classification is at least one of: a public asset, a business confidential asset, a private asset, and a secret asset, wherein said business value of said asset is one of: a low value, a medium value, and a high value, and wherein said resource classification is one of: a trusted classification for internal entities and a non-trusted classification for external entities; and provisioning said computing resource based on said determining step of Gullotta et al. and the results would have been predictable to one of ordinary skill in the art, namely, one skilled in the art would have readily recognized a system and method of virtual provisioning.

Consider claim 17. Gullotta et al. discloses a system configured to facilitate dynamically dynamic provisioning of computing resources (column 13 lines 5-18), said system comprising including a provisioning engine configured to: receive a request for a computing resource, wherein said request is associated with an asset, determine an asset classification, a business value of said asset, and a resource classification related to said asset based upon input from a manager component, wherein said asset classification is at least one of: a public asset, a business confidential asset, a private asset, and a secret asset, wherein said business value of said asset is one of: a low value, a medium value, and a high value, and wherein said resource classification is one of: a trusted classification for internal entities and a non-trusted classification for external entities; and internal entities and a non-trusted classification for external

entities; and provision said computing resource based on said determining step (column 5 lines 13-35, column 18 lines 34-46, column 11 lines 24-52, and column 12 lines 34-53).

Consider claim 9, as applied to claim 1. Gullotta et al. discloses a method comprising de-provisioning said computing resource (Gullotta et al., column 9 lines 47-54).

Consider claim 10, as applied to claim 1. Gullotta et al. discloses a method comprising de-provisioning said computing resource when said computing resource is no longer needed by said asset (Gullotta et al., column 9 lines 47-54).

Consider claim 13, as applied to claim 1. Gullotta et al. discloses a method comprising including defining which processes may be suspended if said asset requires an additional computing resource (Gullotta et al., column 20 lines 23-31).

Consider claim 22, as applied to claim 17. Gullotta et al. discloses a method comprising including a configuration manager instruction module (Gullotta et al., column 15 line 60 – column 16 line 8) configured to identify which processes may be suspended if an asset requires additional computing resource (Gullotta et al., column 20 lines 23-31).

8. Claims 2 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gullotta et al. (US 6985955 B2) in view of Muhlestein et al. (US 20030195942 A1) and in further view of Hartsell et al. (US 20020174227 A!).

Consider claim 2, as applied to claim 1. Gullotta et al., as modified by Muhlestein et al., discloses a computer implemented method for dynamically provisioning computing resources. However, Gullotta et al., as modified by Muhlestein et al., fails to disclose a method including determining a data classification of said asset. Hartsell et al. discloses a method including determining a data classification of said asset (("It will be understood that in the delivery of differentiated services using the disclosed systems and methods, including those illustrated in FIGS. 9A-9D, any packet classification technology (e.g., WAN packet classification technology) that is suitable for classifying or differentiating packets of data may be employed to enable such delivery of differentiated services. Such technologies may be employed to allow the disclosed systems and methods to read incoming packet markings/labels representative of one or more policy-indicative parameters associated with information management policy (e.g., class identification parameters, etc.), to allow the disclosed systems and methods to mark or tag outgoing packets with markings/labels representative of one or more policy-indicative parameters associated with information management policy, or a combination thereof. With regard to packet classification technologies, the disclosed differentiated service functionalities may be implemented using principals that are compatible with, or that apply to, any suitable types of layer two through layer seven packet classification

technologies including, but not limited to, Ethernet 802.1 P/Q, Diffserv, IPv6, MPLS, Integrated Services (RSVP, etc.), ATM QoS, etc. In one embodiment, the disclosed systems and methods may be advantageously enabled to perform such packet classification functionalities by virtue of the presence and functionality of a network interface processing engine as is described in relation to FIGS. 1A and 2 herein.") paragraph 0281).

Therefore, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to incorporate a method including determining a data classification of said asset as taught by Hartsell et al. with a computer implemented method for dynamically provisioning computing resources as taught by Gullotta et al., as modified by Muhlestein et al., for the purpose of QoS provisioning

.

Consider claim 25, as applied to claim 1. Gullotta et al., as modified by Hartsell et al. and Muhlestein et al., discloses a method comprising determining a geographical source from which said request originates (("It will be understood that FIG. 7 illustrates only one exemplary functional representation of an information management system capable of delivering differentiated service, and that differentiated service capability may be implemented in a variety of other ways, using other combinations of the functional components illustrated in FIG. 7, and/or using different functional components and various combinations thereof. For example, operating system 1140 and/or BIOS 1130 may be extended beyond the boundary of system 1110 to deterministically interface

with systems, subsystems or components that are external to system 1110, including systems, subsystems or components that are physically remote from system 1110 (e.g. located in separate chassis, located in separate buildings, located in separate cities/countries etc.) and/or that are not directly coupled to system 1110 through a common distributed interconnect. Examples of such external systems, subsystems or components include, but are not limited to, clustered arrangements of geographically remote or dispersed systems, subsystems or components.") Hartsell et al., paragraph 0259); and applying at least one of a patch or a privacy rule based on said geographical source determination (("The system 10 provides a platform for defining policies and provisioning services to a user interacting with the system, or a user interacting with the network on which the system is operating. The system may designate and track the types of services as well as the types of access to these services for a large number of users. In the generalized examples of FIGS. 1 and 2, the platform system 10 may receive requests for services from user computers. The platform system 10 may also receive information from administrator computers relating to, for example, authorizations of users' requests or changes in users, policies or roles. The platform system 10 may also provide information to the administrator Web browsers or computers, including, for example, reports on operation and service usage. The platform system 10 may provide requests, instructions, or other information to service providers or managed services computers related to providing services to the users, based on user requests, policies, roles, organizational information, and attributes. The platform system 10 may control access to services, such as data, files, programs or other electronic information from

database or storage systems to the users, based on user requests, policies, roles, organizational information, and attributes.") Gullotta et al., column 5 lines 14-35).

9. Claim 11 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gullotta et al. (US 6985955 B2) in view of Muhlestein et al. (US 20030195942 A1) in further view of Torres et al. (US 20050043961 A1) and in further view of Benfield et al. (US 20030009540 A1).

Consider claims 11 and 23, as applied to claims 1 and 17, respectively. Gullotta et al., as modified by Muhlestein et al., discloses a computer implemented method for dynamically provisioning computing resources. However, Gullotta et al., as modified by Muhlestein et al., fails to disclose a method comprising verifying software of at least one of an internal client and external client. Torres et al. discloses a method comprising verifying software of at least one of an internal client and external client (("The present invention is enterprise software that provides a configurable, plug-and-play solution that will search, analyze, and operate on transactional and historical data in real-time across remote and disparate databases. The software has the unique ability to discover similarities and non-obvious relationships in data in real-time and apply the results of data analysis to an operational environment. It has a flexible framework for building a variety of applications that can be configured based on application requirements. Using an open API, the framework enables organizations to easily incorporate multiple

technologies, analytics, software components, and both internal and external data sources. The system performs tasks such as decision automation, transaction processing, and extraction of knowledge from data sources. It can provide the following capabilities: search, analyze, and operate on both transactional and historical data in remote, disparate databases; uncover non-obvious relationships; find similarities as well as exact matches; apply analytical results in an operational environment; easily interoperate with other enterprise applications; combine the results from several different analytics to produce one comprehensive score; search and process large amounts of data in real-time; protect data ownership by using remote search; ensure technology investment due to the ability to easily update and expand the system; operate in serial and parallel environments; protect privacy by returning scores instead of actual data; operate on data with different data types, platforms, and formats; produce a complete audit trail for all search and analytical results; and quickly and easily incorporates multiple analytics, software components, and internal and external data sources. The invention enables more accurate and informed decisions; streamlines operational processes; increases efficiencies and reduces operational costs; transforms data in real-time into useful and useable information; improves customer service and customer interaction; and drives more profitable relationships with customers. It may be used in business-critical applications including employee background checks, risk assessment, fraud detection, data mining, alias identification, market analysis, and customer identification. Modular software components provide unique analytical capabilities such as link analysis, fuzzy search, similarity scoring and classifications,

and rules processing as well as a complete decision audit trail. The invention also accepts and integrates third party analytics and software components.") paragraph 0020). Therefore, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to incorporate a method including verifying software of at least one of an internal client and external client as taught by Torres et al. with a computer implemented method for dynamically provisioning computing resources as taught by Gullotta et al., as modified by Muhlestein et al., for the purpose of application-aware provisioning. However, Gullotta et al., as modified by Muhlestein et al. and Torres et al., fails to disclose a method of taking inventory of an internal and an external network. Benfield et al. discloses a method of taking inventory of an internal and an external network (("While firewalls may prevent certain entities from obtaining information from the protected internal network, firewalls may also present a barrier to the operation of legitimate, useful processes. For example, in order to ensure a predetermined level of service, benevolent processes may need to operate on both the external network and the protected internal network; a customer system is more efficiently managed if the management software can dynamically detect and dynamically configure hardware resources as they are installed, rebooted, etc. Various types of discovery processes, status polling, status gathering, etc., may be used to get information about the customer's large, dynamic, distributed processing system. This information is then used to ensure that quality-of-service guarantees to the customer are being fulfilled. However, firewalls might block these system processes, especially discovery processes.") paragraph 0202).

Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate a method of taking inventory of an internal and an external network as taught by Benfield with a method including verifying software of at least one of an internal client and external client and a computer implemented method for dynamically provisioning computing resources as taught by Gullotta et al., as modified by Muhlestein et al. and Torres et al., for the purpose of identity management.

10. Claims 12 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gullotta et al. (US 6985955 B2) in view of Muhlestein et al. (US 20030195942 A1) and in further view of Oren et al. (US 20030145093 A1).

Consider claims 12 and 21, as applied to claims 1 and 17, respectively. Gullotta et al., as modified by Muhlestein et al., discloses a computer implemented method for dynamically provisioning computing resources. However, Gullotta et al., as modified by Muhlestein et al., fails to disclose a method comprising an instruction module configured to apply encryption to asset data based on said asset classification. Oren et al. discloses a method comprising applying encryption to asset data based on said asset classification ((“According to optional but preferred embodiments of the present invention, system 10 also features an information security system for encrypting and/or authenticating classified data defined by the user before transmitting such data from

peer device 12 of the user. Client module 14 is preferably able to manage renewed sets of security keys which are downloaded from central location authority, and particularly from a server which acts as the certificate authority of system 10.") paragraph 0083).

Therefore, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to incorporate a method including applying encryption to asset data based on said asset classification as taught by Oren et al. with a computer implemented method for dynamically provisioning computing resources as taught by Gullotta et al., as modified by Muhlestein et al., for the purpose of thin provisioning and data classification.

11. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gullotta et al. (US 6985955 B2) in view of Muhlestein et al. (US 20030195942 A1) and in further view of Grannon (US 20050010671 A1).

Consider claim 15, as applied to claim 1. Gullotta et al., as modified by Muhlestein et al., discloses a computer implemented method for dynamically provisioning computing resources. However, Gullotta et al., as modified by Muhlestein et al., fails to disclose a method comprising storing policies regarding processing assets when computing resources are limited due to a failure of at least one of software and hardware. Grannon discloses a method comprising storing policies regarding processing assets when computing resources are limited due to a failure of at least one

of software and hardware ((“For purposes of illustration and example, the MMS software 188 configures itself to be a slave server for redundancy within the premises in response to detecting an existing MMS module (namely the MMS software 120) in another device (namely the personal computer 110). Thus, while the MMS software 120 in the personal computer 110 is functioning properly and providing server functions, the STB 180 functions as an MMC device. However, the STB 180 keeps a copy of media asset and device profile tables to account for which media files are stored on all of the devices and how associated memory across the devices is allocated. The STB 180 keeps the tables in order to take over as the MMS if the personal computer 110 should fail. Also for redundancy purposes, the MMS software 120 can manage data replication across multiple devices to ensure that identical pieces of data are stored on different devices.”) paragraph 0026).

Therefore, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to incorporate a method including storing policies regarding processing assets when computing resources are limited due to failures of at least one of software and hardware as taught by Grannon with a computer implemented method for dynamically provisioning computing resources as taught by Gullotta et al., as modified by Muhlestein et al., for the purpose of application-aware storage.

12. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gullotta et al. (US 6985955 B2) in view of Muhlestein et al. (US 20030195942 A1) and in further view of Tredoux et al. (US 20020161904 A1).

Consider claim 18, as applied to claim 17. Gullotta et al., as modified by Muhlestein et al., discloses a computer implemented method for dynamically provisioning computing resources. However, Gullotta et al., as modified by Muhlestein et al., fails to disclose a system comprising a server configured to communicate with at least one of an internal and external client. Tredoux et al. discloses a system comprising a server configured to communicate with at least one of an internal and external client (("No assumptions need be rendered regarding the network protocol used by the external network device client to communicate with the internal network device and/or (hidden) server on the protected network. All network traffic, for example TCP/IP traffic, is tunneled by the proxy agent 240 through the exemplary HTTP connection between the proxy agent 240 and the external proxy server 250, and there is generally no need for them to alter this data, with some notable exceptions. Certain protocols can require special treatment, particularly HTTP itself. The use of embedded hyperlinks in HTML pages implies that a client may be redirected by a link to an inaccessible URL hidden behind the security device/firewall 20, away from the external proxy server 250 which enables its access to the hidden network. To prevent or minimize such undesirable redirection, a web browser / external device 230 can be configured (through standard browser settings) to use the external proxy server 250 as a true HTTP proxy server,

using the local port on the server described above. This ensures that all HTTP requests are forwarded intact and uninterpreted to the external proxy server 250, which passes those requests to the proxy agent 240. The agent 240 retrieves the requested URLs, which are directly accessible to it since it is behind the firewall 20.") paragraph 0033).

Therefore, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to incorporate a system including a server configured to communicate with at least one of an internal and external client as taught by Tredoux et al. with a computer implemented method for dynamically provisioning computing resources as taught by Gullotta et al., as modified by Muhlestein et al., for the purpose of class-based provisioning.

13. Claims 19 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gullotta et al. (US 6985955 B2) in view of Muhlestein et al. (US 20030195942 A1) and in further view of Elliot et al. (US 20020064149 A1).

Consider claims 19 and 24, as applied to claim 17. Gullotta et al., as modified by Muhlestein et al., discloses a computer implemented method for dynamically provisioning computing resources. However, Gullotta et al., as modified by Muhlestein et al., fails to disclose a system comprising a domain database configured to store domain rules and policies. Elliot et al. discloses a system comprising a domain database configured to store domain rules and policies ((“Data recovery of failed

databases is needed in real time.") paragraph 0757 ("Data Administration (dbAdmin) 2238 involves setting data policy, managing the logical and physical aspect of the databases, and securing and configuring the functional components of the Data Management 2138 domain. Data Management policies include security, distribution, integrity rules, performance requirements, and control of replications and partitions. dbAdmin 2238 includes the physical control of data resources such as establishing data locations, allocating physical storage, allocating memory, loading data stores, optimizing access paths, and fixing database problems. dbAdmin 2238 also provides for logical control of data such as auditing, reconciling, migrating, cataloguing, and converting data.") paragraph 1002).

Therefore, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to incorporate a system including a domain database configured to store domain rules and policies as taught by Elliot et al. with a computer implemented method for dynamically provisioning computing resources as taught by Gullotta et al., as modified by Muhlestein et al., for the purpose of a classification database.

14. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Gullotta et al. (US 6985955 B2) in view of Muhlestein et al. (US 20030195942 A1) and in further view of Baba et al. (US 20060168253 A1).

Consider claim 20, as applied to claim 17. Gullotta et al., as modified by Muhlestein et al., discloses a computer implemented method for dynamically provisioning computing resources. However, Gullotta et al., as modified by Muhlestein et al., fails to disclose a system comprising a connection manager configured to direct at least one of an internal client and external client to comply with software requirements. Baba et al. discloses a system comprising a connection manager configured to direct at least one of an internal client and external client to comply with software requirements (("An application gateway 110 having a firewall function of limiting accesses from devices connected to the external network 120 is provided between the external network 120 and the internal network constituted of the home network 100. The application gateway checks a communication packet in an application layer upon receiving an access request from the external network so as to perform filtering.") paragraph 0097).

Therefore, it would have been obvious for a person of ordinary skill in the art at the time the invention was made to incorporate a system including a connection manager configured to direct at least one of an internal client and external client to comply with software requirements as taught by Baba et al. with a computer implemented method for dynamically provisioning computing resources as taught by Gullotta et al., as modified by Muhlestein et al., for the purpose of class-based provisioning.

Response to Arguments

15. Applicant's arguments filed 02 March 2009 with respect to claims 1-2 and 16-17 have been considered but are not persuasive.

Applicant argues that Gullotta et al., as modified by Muhlestein et al., fails to disclose "assigning said asset to one of a plurality of security domains based on said determining (determining an asset classification), wherein each security domain corresponds to a respective degree of security control," as claimed in Claim 1.

Examiner respectfully disagrees. Gullotta et al., as modified by Muhlestein et al., discloses a system and method comprising security domains (("An architecture provides the ability to create and maintain multiple instances of virtual servers, such as virtual filers (vfilers), within a server, such as a filer. A vfiler is a logical partitioning of network and storage resources of the filer platform to establish an instance of a multi-protocol server. Each vfiler is allocated a subset of dedicated units of storage resources, such as volumes or logical sub-volumes (qtrees), and one or more network address resources. Each vfiler is also allowed shared access to a file system resource of a storage operating system. To ensure controlled access to the allocated and shared resources, each vfiler is further assigned its own security domain for each access protocol. A vfiler boundary check is performed by the file system to verify that a current vfiler is allowed to access certain storage resources for a requested file stored on the filer platform.") Muhlestein et al., abstract); security control policies across said domains (("In this manner, the interfaces to external clients and systems are isolated to one or more

servers containing only those components of the system necessary for external interface. Other components of the system, including, but not limited to, those components that must remain secure, may reside on servers that do not interface to external clients and servers. Thus, external users of the system whose trustworthiness has not been verified are isolated from secure portions of the system, and the integrity of secure portions of the system residing on other servers within the system may be protected.") Gullotta et al., column 16 lines 44-54 ("An External Data Input functional area may group all requirements for incorporating current customer information into the system, such as existing users and resources. An Organization Management functional area may group all requirements for adding, modifying, and deleting organizations. A Policy Based Provisioning functional area may group all requirements for defining the provisioning of services based on attributes or a users' membership in a role, group, organizational unit, or organization.") Gullotta et al., column 17 lines 10-18 ("FIG. 7E is a sequence diagram of interactions for implementing an addition of a user to the system and provisioning of services for that user based on provisioning policies. In embodiments of the present invention, user provisioning is accomplished with the RPM system described hereinabove. Unlike RBAC, which provisions users with "soft" resources (such as accounts) based on only on roles, RPM provisions users with both "hard" and "soft" resources based on policies, which are defined according to user roles and attributes.") Gullotta et al., column 17 lines 50-58); and determining association (read as classifications) (("The user applications 110 may also include a Policy Management application 128 that provides an interface for defining policies that control

the provisioning of services to users. In addition, constraints on individual attributes of services may be defined. The policies determine an association between the users and the services or resources, and constraints on those services provisioned to the users, based on attributes and user roles. The policies may define one or a series of approvals that are required before provisioning a given service or any service to a user. For example, such approvals may be required from one or more other users acting in a supervisory role. Policies may require one or more approvals if an attribute constraint is violated. The approvals may be defined using a Workflow Management application 130, which provides an interface for defining the approval process needed for a request in the system. As described above, the platform subsystem 104 includes service and utility modules that enable various applications of the system to interact with directories and databases that hold information relating to the state of the system and services available over the network. The platform subsystem 104 may include, for example, application services 132, data services 134 and remote services 136. In preferred embodiments, the platform modules are designed to be as independent as possible of any domain-specific information. This enables the platform to be easily applied to a different domain and support a new set of applications without (or with minimal) re-architecture.") Gullotta et al., column 11 lines 37-64).

Applicant argues that Gullotta et al., as modified by Muhlestein et al., fails to disclose "assigning the asset to one of a plurality of security domains based on a determining step" (determining an asset classification).

Examiner respectfully disagrees. Gullotta et al., as modified by Muhlestein et al., discloses a system and method comprising a plurality of security domains (("An architecture provides the ability to create and maintain multiple instances of virtual servers, such as virtual filers (vfilers), within a server, such as a filer. A vfiler is a logical partitioning of network and storage resources of the filer platform to establish an instance of a multi-protocol server. Each vfiler is allocated a subset of dedicated units of storage resources, such as volumes or logical sub-volumes (qtrees), and one or more network address resources. Each vfiler is also allowed shared access to a file system resource of a storage operating system. To ensure controlled access to the allocated and shared resources, each vfiler is further assigned its own security domain for each access protocol. A vfiler boundary check is performed by the file system to verify that a current vfiler is allowed to access certain storage resources for a requested file stored on the filer platform.") Muhlestein et al., abstract); and determining an association (read as classification) (("These and other advantages are accomplished according to a method and system for provisioning users with resources. A method for provisioning users with resources is disclosed. The method includes the steps of establishing a set of attributes, organizational information, and user roles and defining a plurality of resource provisioning policies based on selected attributes, organizational information, and user roles. The method also includes the steps of receiving attribute information and user role information for a particular user or resource, determining which resource provisioning policies are applicable to the user based on the received user role

information, organizational information, and attribute information, seeking additional information or authorizations from third parties in accordance with the applicable resource provisioning policies, and provisioning the user with the resources specified by the applicable resource provisioning policies if all necessary additional information or authorizations have been received from the third parties.") Gullotta et al., column 2 line 59 – column 3 line 10 ("The user applications 110 may also include a Policy Management application 128 that provides an interface for defining policies that control the provisioning of services to users. In addition, constraints on individual attributes of services may be defined. The policies determine an association between the users and the services or resources, and constraints on those services provisioned to the users, based on attributes and user roles. The policies may define one or a series of approvals that are required before provisioning a given service or any service to a user. For example, such approvals may be required from one or more other users acting in a supervisory role. Policies may require one or more approvals if an attribute constraint is violated. The approvals may be defined using a Workflow Management application 130, which provides an interface for defining the approval process needed for a request in the system.") Gullotta et al., column 11 lines 37-52).

Conclusion

16. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any response to this Office Action should be faxed to (571) 273-8300 or mailed to:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Mark Fearer whose telephone number is (571) 270-1770. The Examiner can normally be reached on Monday-Thursday from 7:30am to 5:00pm.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Tonia Dollinger can be reached on (571) 272-4170. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free) or 571-272-4100.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist/customer service whose telephone number is (571) 272-2600.

Mark Fearer
/M.D.F./
May 14, 2009

/George C Neurauter, Jr./

Primary Examiner, Art Unit 2443